

WO 2005/008385 A3

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization International Bureau



(43) International Publication Date
27 January 2005 (27.01.2005)

PCT

(10) International Publication Number
WO 2005/008385 A3

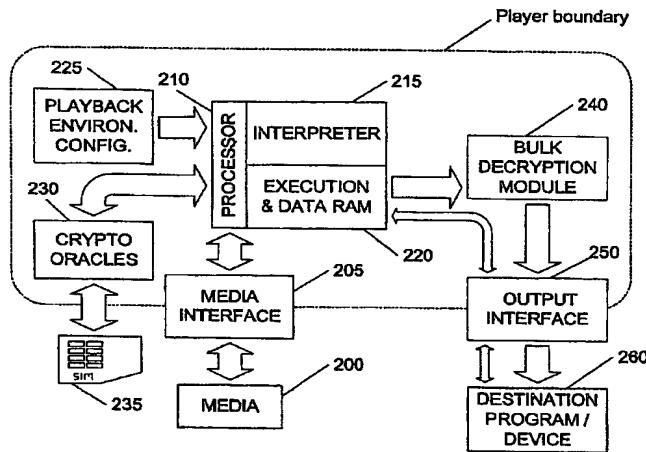
- (51) International Patent Classification⁷: **G06F 12/14**
- (21) International Application Number:
PCT/US2004/021621
- (22) International Filing Date: 7 July 2004 (07.07.2004)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
10/614,765 7 July 2003 (07.07.2003) US
60/537,421 16 January 2004 (16.01.2004) US
- (71) Applicant (for all designated States except US): **CRYPTOGRAPHY RESEARCH, INC.** [US/US]; 575 Market Street, Suite 2150, San Francisco, CA 94105 (US).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): **KOCHER, Paul, C.** [US/US]; 134 Fillmore Street, San Francisco, CA 94117 (US). **JAFFE, Joshua, M.** [US/US]; 1833 Church Street, San Francisco, CA 94131 (US). **JUN, Benjamin, C.** [US/US]; 133 Duncan Street, San Francisco, CA 94110 (US). **LAREN, Carter, C.** [US/US]; 86 Barcelona Avenue, San Francisco, CA 94115 (US). **PEARSON, Peter, K.** [US/US]; 5624 Victoria Lane, Livermore, CA 94550 (US).
- (74) Agent: **RADLO, Edward, J.; Sonnenschein, Nath & Rosenthal**, Post Office Box 61080, Wacker Drive Station, Sears Tower, Chicago, IL 60606 (US).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report

[Continued on next page]

(54) Title: REPROGRAMMABLE SECURITY FOR CONTROLLING PIRACY AND ENABLING INTERACTIVE CONTENT



(57) Abstract: Technologies are disclosed to transfer responsibility and control over security from player makers to content authors by enabling integration of security logic and content. An exemplary optical disk (200) carries an encrypted digital video title combined with data processing operations (225) that implement the titles security policies and decryption processes. Player devices include a processing environment (e.g., a real-time virtual machine), which plays content by interpreting its processing operations. Players also provide procedure calls to enable content code to load data from media, perform network communications, determine playback environment configurations (225), access secure non-volatile storage, submit data to CODECs for output (250), and/or perform cryptographic operations. Content can insert forensic watermarks in decoded output for tracing pirate copies. If pirates compromise a player or title, future content can be mastered with security features that, for example, block the attack, revoke pirated media, or use native code to correct player vulnerabilities.



— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(88) Date of publication of the international search report:
19 May 2005